UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/435,899	11/08/1999	PAUL JOSEPH SEGER	TU999050	5856

7590	07/12/2006

JOHN H. HOLCOMBE
INTELLECTUAL PROPERTY LAW
8987 E. TANQUE VERDE RD. #309-374
TUCSON, AZ 85749-9610

EXAMINER
BETIT, JACOB F

ART UNIT	PAPER NUMBER
2164	

DATE MAILED: 07/12/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

	Application No.	**Applicant(s)**
Office Action Summary	09/435,899	SEGER, PAUL JOSEPH
	Examiner	**Art Unit**	
	Jacob F. Betit	2164	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10 April 2006*.

2a)☒ This action is **FINAL.**   2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-50* is/are pending in the application.

   4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) *29-39* is/are allowed.

6)☒ Claim(s) *1-28 and 40-50* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

   Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

   Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   a)☐ All   b)☐ Some * c)☐ None of:

   1.☐ Certified copies of the priority documents have been received.

   2.☐ Certified copies of the priority documents have been received in Application No. _____.

   3.☐ Copies of the certified copies of the priority documents have been received in this National Stage
   application from the International Bureau (PCT Rule 17.2(a)).

   * See the attached detailed Office action for a list of the certified copies not received.

SAM RIMELL
PRIMARY EXAMINER

Attachment(s)

1)☐ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date *1/23/06*.

4)☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5)☐ Notice of Informal Patent Application (PTO-152)

6)☐ Other: _____.

Remarks

1.   In response to communications filed on 10 April 2006 and 5 December 2005

claims 1-66 are presently pending in the application, claims 51-66 are withdrawn from

further consideration. Claims 1, 15, 29, and 40 are amended per applicant's request

Election/Restrictions

2.   Applicant's election without traverse of Group I claims 1-50 in the reply filed on

10 April 2006 is acknowledged.

Claim Rejections - 35 USC § 112

3.   The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

4.   Claims 40-50 rejected under 35 U.S.C. 112, second paragraph, as being indefinite

for failing to particularly point out and distinctly claim the subject matter which applicant

regards as the invention.

5.   Claim 40 recites the limitation "having data storage media", in line 4, and the

limitations "having data storage media" in line 7. It is not clear from reading the

limitations if both of these "data storage media" are the same or different storage media.

Therefore, later limitations referring to "said data storage media" are indefinite.

Claim Rejections - 35 USC § 103

6.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7.   Claims 1, 6, 8-9, 15, 20, 22-23, 29, 40, 44, and 46 are rejected under 35 U.S.C.

103(a) as being unpatentable over <u>Anderl et al.</u> (International Publication No. 87/07062)

in view of <u>Smith</u> (U.S. patent No. 4,9563,769).

As to claim 1, <u>Anderl et al.</u> teaches a portable security system for managing

access to a portable data storage cartridge, the data storage cartridge having data storage

media for storing data for read/write access by a user of a data storage drive when

mounted in the data storage drive (see abstract), the portable security system comprising:

a wireless interface mounted in the portable data storage cartridge for receiving

power and data from, and sending data to, the data storage drive when mounted in the

data storage drive (see page 5, line 31 through page 6, line 23); and

a computer processor mounted in the portable data storage cartridge separate from

said data storage media, and coupled to the wireless interface (see figure 1, reference

numbers 110, 115, 120, and 130); the computer processor powered by the wireless

interface and receiving and transmitting data to the data storage drive via the wireless

interface (see page 5, line 31 through page 6, line 23); the computer processor receiving

the user authentication messages from the data storage drive via the wireless interface,

and transmitting the user authorization or denial to the data storage drive via the wireless

interface (see page 10, lines 19-26).

Anderl et al. does not teach the computer processor having a user table

comprising at least a unique user identifier for each authorized user and at least one

permitted activity the user is authorized to conduct with respect to the data storage media,

the user identifier, when combined with a user authentication message from the

authorized user in accordance with a predetermined algorithm, authorizes the user; and

combining the user authentication message with at least part of the user identifier from

the user table in accordance with the predetermined algorithm to authorize or deny the

user activity.

Smith teaches a security system for computer databases (see abstract), in which he

teaches the computer processor having a user table comprising at least a unique user

identifier for each authorized user and at least one permitted activity the user is

authorized to conduct with respect to the data storage media (see column 2, lines 11-17),

the user identifier, when combined with a user authentication message from the

authorized user in accordance with a predetermined algorithm, authorizes the user (see

column 5, lines 9-14 and see figure 1); and combining the user authentication message

with at least part of the user identifier from the user table in accordance with the

predetermined algorithm to authorize or deny the user activity (see column 5, lines 9-14

and see figure 1).

It would have been obvious to a person having ordinary skill in the art at the time

the invention was made to have modified Anderl et al. by the teachings of Smith because

the computer processor having a user table comprising at least a unique user identifier for

each authorized user and at least one permitted activity the user is authorized to conduct

with respect to the data storage media, the user identifier, when combined with a user

authentication message from the authorized user in accordance with a predetermined

algorithm, authorizes the user; and combining the user authentication message with at

least part of the user identifier from the user table in accordance with the predetermined

algorithm to authorize or deny the user activity would limit the access of selected users to

pre-selected locations which they are authorized to access (see Smith, column 1, lines 7-

12).

As to claim 15, Anderl et al. teaches a data storage cartridge for storing data for

read/write access by a user of a data storage drive when mounted in the data storage drive

(see abstract), comprising:

data storage media mounted in the data storage cartridge for storing the data for

the read/write access (see figure 1, reference number 115); a wireless interface mounted

in the portable data storage cartridge for receiving power and data from, and sending data

to, the data storage drive when mounted in the data storage drive (see page 5, line 31

through page 6, line 23); and

a computer processor mounted in the portable data storage cartridge separate from

said data storage media, and coupled to the wireless interface (see figure 1, reference

numbers 110, 115, 120, and 130); the computer processor powered by the wireless

interface and receiving and transmitting data to the data storage drive via the wireless

interface (see page 5, line 31 through page 6, line 23); the computer processor receiving

the user authentication messages from the data storage drive via the wireless interface,

and transmitting the user authorization or denial to the data storage drive via the wireless

interface (see page 10, lines 19-26).

Anderl et al. does not teach the computer processor having a user table

comprising at least a unique user identifier for each authorized user and at least one

permitted activity the user is authorized to conduct with respect to the data storage media,

the user identifier, when combined with a user authentication message from the

authorized user in accordance with a predetermined algorithm, authorizes the user; and

combining the user authentication message with at least part of the user identifier from

the user table in accordance with the predetermined algorithm to authorize or deny the

user activity.

Smith teaches the computer processor having a user table comprising at least a

unique user identifier for each authorized user and at least one permitted activity the user

is authorized to conduct with respect to the data storage media (see column 2, lines 11-

17), the user identifier, when combined with a user authentication message from the

authorized user in accordance with a predetermined algorithm, authorizes the user (see

column 5, lines 9-14 and see figure 1); and combining the user authentication message

with at least part of the user identifier from the user table in accordance with the

predetermined algorithm to authorize or deny the user activity (see column 5, lines 9-14

and see figure 1).

It would have been obvious to a person having ordinary skill in the art at the time

the invention was made to have modified Anderl et al. by the teachings of Smith because

the computer processor having a user table comprising at least a unique user identifier for

each authorized user and at least one permitted activity the user is authorized to conduct

with respect to the data storage media, the user identifier, when combined with a user

authentication message from the authorized user in accordance with a predetermined

algorithm, authorizes the user; and combining the user authentication message with at

least part of the user identifier from the user table in accordance with the predetermined

algorithm to authorize or deny the user activity would limit the access of selected users

to pre-selected locations which they are authorized to access (see Smith, column 1, lines

7-12).

As to claim 40, Anderl et al. teaches a computer program product usable with a

programmable computer processor having computer readable program code embodied

therein for providing a secure interface to a data storage cartridge having data storage

media (see abstract), the programmable computer processor mounted in the data storage

cartridge separate from said data storage media (see figure 1, reference number 110 and

115), the data storage cartridge having data storage media for storing data for read/write

access by a user of a data storage drive when mounted in the data storage drive (see

figure 1, reference number 115), and a wireless interface mounted in the portable data

storage cartridge for receiving power and data from, and sending data to, the data storage

drive when mounted in the data storage drive (see page 5, line 31 through page 6, line

23), the computer program product comprising:

computer readable program code which causes the programmable computer

processor to, separate from said data storage media, receive the user authentication

messages from the data storage drive via the wireless interface; and computer readable

program code which causes the programmable computer processor to transmit the user

authorization or denial to the data storage drive via the wireless interface (see page 10,

lines 19-26).

Anderl et al. does not teach computer readable program code which causes the

programmable computer processor to provide a user table comprising at least a unique

user identifier for each authorized user and at least one permitted activity the user is

authorized to conduct with respect to the data storage media, the user identifier, when

combined with a user authentication message from the authorized user in accordance with

a predetermined algorithm, authorizes the user; and combine the user authentication

message with at least part of the user identifier from the user table in accordance with the

predetermined algorithm to authorize or deny the user activity.

Smith teaches computer readable program code which causes the programmable

computer processor to provide a user table comprising at least a unique user identifier for

each authorized user and at least one permitted activity the user is authorized to conduct

with respect to the data storage media (see column 2, lines 11-17), the user identifier,

when combined with a user authentication message from the authorized user in

accordance with a predetermined algorithm, authorizes the user (see column 5, lines 9-14

and see figure 1); and computer readable program code which causes the programmable

computer processor to combine the user authentication message with at least part of the

user identifier from the user table in accordance with the predetermined algorithm to

authorize or deny the user activity (see column 5, lines 9-14 and see figure 1).

It would have been obvious to a person having ordinary skill in the art at the time

the invention was made to have modified Anderl et al. by the teachings of Smith because

computer readable program code which causes the programmable computer processor to

provide a user table comprising at least a unique user identifier for each authorized user

and at least one permitted activity the user is authorized to conduct with respect to the

data storage media, the user identifier, when combined with a user authentication

message from the authorized user in accordance with a predetermined algorithm,

authorizes the user; and computer readable program code which causes the

programmable computer processor to combine the user authentication message with at

least part of the user identifier from the user table in accordance with the predetermined

algorithm to authorize or deny the user activity would limit the access of selected users to

pre-selected locations which they are authorized to access (see Smith, column 1, lines 7-

12).

As to claims 6, 20, and 44, Anderl et al. as modified, teaches wherein the

computer processor user table permitted activities comprise a plurality of permitted

activities, selected ones of which each of the users may be authorized to conduct, the

permitted activities comprising 1) read access to data stored in the data storage media, 2)

write access to data stored in the data storage media (see Smith, column 4, lines 59-66),

3) read the user entry of the user table, 4) read all entries of the user table, 5) add entries

to the user table, and 6) change/delete entries to the user table (see Smith, column 3, line

62 through column 4, line 14).

As to claims 8, 22, and 46, Anderl et al. as modified, teaches wherein the

computer processor user table comprises a separate entry for each the user identifier, the

entry comprising all the permitted activities the user is authorized to conduct (see Smith,

column 2, lines 11-17).

As to claims 9 and 23, <u>Anderl et al.</u> as modified, teaches wherein the computer processor additionally comprises a nonvolatile memory storing the user table (see <u>Anderl et al.</u>, page 11, lines 21-26).

8.   Claims 2 and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over <u>Anderl et al.</u> (International Publication No. 87/07062) in view of <u>Smith</u> (U.S. patent No. 4,9563,769) as applied to claims 1, 6, 8-9, 15, 20, 22-23, 29, 40, 44, and 46 above, and further in view of <u>Davis</u> (U.S. patent No. 4,941,201).

As to claims 2 and 16, <u>Anderl et al.</u> as modified, does not teach wherein the wireless interface comprises an RF interface.

<u>Davis</u> teaches an electronic data storage apparatus (see abstract), in which he teaches wherein the wireless interface comprises an RF interface (see column 5, lines 55-61 and see column 21, lines 31-46, where 100 kHz is in the RF range of the Electromagnetic Spectrum).

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified <u>Anderl et al.</u> as modified, by the teachings of <u>Davis</u> because wherein the wireless interface comprises an RF interface would make the propagation delay between the outputs of the inverters 5 microseconds (see <u>Davis</u>, column 21, lines 39-46).

9.   Claims 3-5, 17-19, and 41-43 are rejected under 35 U.S.C. 103(a) as being unpatentable over <u>Anderl et al.</u> (International Publication No. 87/07062) in view of <u>Smith</u>

(U.S. patent No. 4,9563,769) as applied to claims 1, 6, 8-9, 15, 20, 22-23, 29, 40, 44, and

46 above, and further in view of Wright et al. (U.S. patent No. 6,084,969).

As to claims 3, 17, and 41, Anderl et al. as modified, does not teach wherein each

the user identifier comprises a user symbol and a user decrypting key, wherein the user

authentication message comprises an encrypted user authentication message which may

be decrypted by the user decrypting key, and wherein the computer processor conducts

the combination by decrypting the user authentication message by the user decrypting

key.

Wright et al. teaches an encryption system for a two way pager (see abstract), in

which he teaches wherein each the user identifier comprises a user symbol and a user

decrypting key (see column 11, line 65 through column 12, line 5), wherein the user

authentication message comprises an encrypted user authentication message which may

be decrypted by the user decrypting key, and wherein the computer processor conducts

the combination by decrypting the user authentication message by the user decrypting

key (see column 12, lines 5-13).

It would have been obvious to a person having ordinary skill in the art at the time

the invention was made to have modified Anderl et al. as modified, by the teachings of

Wright et al. because wherein each the user identifier comprises a user symbol and a user

decrypting key, wherein the user authentication message comprises an encrypted user

authentication message which may be decrypted by the user decrypting key, and wherein

the computer processor conducts the combination by decrypting the user authentication

message by the user decrypting key would authenticate the sender and protect the

contents of the message (see <u>Wright et al.</u>, column 9, lines 51-56).

As to claims 4, 18, and 42, <u>Anderl et al.</u> as modified, teaches wherein the user

decrypting key comprises a sender public key, and wherein the predetermined algorithm

comprises a public key cryptographic algorithm (see <u>Wright et al.</u>, column 12, lines 5-

13).

As to claims 5 and 19, <u>Anderl et al.</u> as modified, teaches wherein the user

authentication message is encrypted by a sender private key and a receiver public key

(see <u>Wright et al.</u>, column 9, lines 51-56), and wherein the public key cryptographic

algorithm decrypts the user authentication message employing a receiver private key and

the sender public key, whereby the user authentication message is known to have come

from the user (see <u>Wright et al.</u>, column 12, lines 5-13).

As to claim 43, <u>Anderl et al.</u> as modified, teaches wherein the user authentication

message is encrypted by a sender private key and a receiver public key (see <u>Wright et al.</u>,

column 9, lines 51-56), wherein the public key cryptographic algorithm decrypts the user

authentication message employing a receiver private key and the sender public key, and

wherein the combining step comprises decrypting the user authentication message by the

receiver private key and the sender public key, whereby the user authentication message

is known to have come from the user (see <u>Wright et al.</u>, column 12, lines 5-13).

1.   Claims 7, 10-13, 21, 24-27, 45, and 47-49 rejected under 35 U.S.C. 103(a) as

being unpatentable over <u>Anderl et al.</u> (International Publication No. 87/07062) in view of

<u>Smith</u> (U.S. patent No. 4,9563,769) as applied to claims 1, 6, 8-9, 15, 20, 22-23, 29, 40,

44, and 46 above, and further in view of <u>Bapat et al.</u> (U.S. patent No. 6,038,563).

        As to claims 7, 21, and 45, <u>Anderl et al.</u> as modified, does not teach wherein the

computer processor user table comprises a separate entry for each the user identifier and

the permitted activity the user is authorized to conduct.

        <u>Bapat et al.</u> teaches access control to a database using a permissions table (see

abstract), in which he teaches wherein the computer processor user table comprises a

separate entry for each the user identifier and the permitted activity the user is authorized

to conduct.

        It would have been obvious to a person having ordinary skill in the art at the time

the invention was made to have modified <u>Anderl et al.</u> as modified, by the teachings of

<u>Bapat et al.</u> because wherein the computer processor user table comprises a separate entry

for each the user identifier and the permitted activity the user is authorized to conduct

would give a way to grant or deny access to certain users (see <u>Bapat et al.</u>, column 11,

lines 4-7).

        As to claims 10, 24, and 47, <u>Anderl et al.</u> as modified, teaches receiving the user

authentication messages from the data storage drive via the wireless interface, and

transmitting the class authorization or denial to the data storage drive via the wireless

interface (see <u>Anderl et al.</u> page 12, lines 7-15, and see figure 7).

Anderl et al. as modified, does not teach wherein the computer processor

additionally comprises a class table comprising at least a unique class identifier for each

authorized class of users and at least one permitted activity the class of users is

authorized to conduct with respect to the data storage media, the class identifier, when

combined with a user authentication message from a user of the authorized class of users

in accordance with the predetermined algorithm, authorizes the user; and wherein the

computer processor additionally, upon receiving the user authentication messages,

combining the user authentication message with the class identifier from the class table in

accordance with the predetermined algorithm to authorize or deny the class activity to the

user, and transmitting the class authorization or denial.

Bapat et al. teaches wherein the computer processor additionally comprises a class

table comprising at least a unique class identifier for each authorized class of users and at

least one permitted activity the class of users is authorized to conduct with respect to the

data storage media, the class identifier (see column 10, lines 35-47), when combined with

a user authentication message from a user of the authorized class of users in accordance

with the predetermined algorithm, authorizes the user (see figure 5); and wherein the

computer processor additionally, upon receiving the user authentication messages,

combining the user authentication message with the class identifier from the class table in

accordance with the predetermined algorithm to authorize or deny the class activity to the

user, and transmitting the class authorization or denial (see figure 6).

It would have been obvious to a person having ordinary skill in the art at the time

the invention was made to have modified Anderl et al. as modified, by the teachings of

Bapat et al. because wherein the computer processor additionally comprises a class table

comprising at least a unique class identifier for each authorized class of users and at least

one permitted activity the class of users is authorized to conduct with respect to the data

storage media, the class identifier, when combined with a user authentication message

from a user of the authorized class of users in accordance with the predetermined

algorithm, authorizes the user; and wherein the computer processor additionally, upon

receiving the user authentication messages, combining the user authentication message

with the class identifier from the class table in accordance with the predetermined

algorithm to authorize or deny the class activity to the user, and transmitting the class

authorization or denial would make an easy way to define a set of access rules to grant

access rights to a broad group of users (see Bapat et al., column 11, lines 56-59) and

would help to reduce the amount of data required to define access rules (see Bapat et al.,

column 9, lines 48-50).

As to claims 11, 25, and 48, Anderl et al. as modified, teaches wherein the

computer processor user table additionally comprises any class membership of each the

user (see Bapat et al., Column 10, lines 4-10), wherein the user may be authorized with

respect to the class table either by the class authorization or by the user authorization (see

Bapat et al., figure 15A).

As to claims 12, 26, and 49, Anderl et al. as modified, teaches wherein the

computer processor user table and the class table permitted activities comprise a plurality

of permitted activities, selected ones of which each of the users may be authorized to

conduct, the permitted activities comprising 1) read access to data stored in the data

storage media, 2) write access to data stored in the data storage media, 3) read all entries

of the class table, 4) add entries to the class table, and 5) change/delete entries to the class

table (see Bapat et al., column 10, lines 35-47).

As to claims 13 and 27, Anderl et al. as modified, teaches wherein the computer

processor additionally comprises a 'nonvolatile memory storing the user table (see Anderl

et al., page 11, lines 14-26) and the class table (see Bapat et al., column 7, lines 18-24).

2.   Claims 14, 28, and 50 are rejected under 35 U.S.C. 103(a) as being unpatentable

over Anderl et al. (International Publication No. 87/07062) in view of Smith (U.S. patent

No. 4,9563,769) as applied to claims 1, 6, 8-9, 15, 20, 22-23, 29, 40, 44, and 46 above,

and further in view of Hastings et al. (U.S. patent No. 6,370,629 B1).

As to claims 14, 28, and 50 Anderl et al. as modified, teaches wherein the

computer processor user table permitted activities comprise at least 1) read access to data

stored in the data storage media (see Smith, column 4, lines 59-66).

Anderl et al. as modified, does not teach wherein the data stored in the data

storage media is encrypted, and wherein the user authorization for the read access

additionally comprises a decryption key for the encrypted stored data.

Hastings et al. teaches giving access to information based on time and geographic

position (see abstract), in which he teaches wherein the data stored in the data storage

media is encrypted (see column 3, line 63 through column 4, line 4), and wherein the user

authorization for the read access additionally comprises a decryption key for the

encrypted stored data (see column 5, lines 52-61).

It would have been obvious to a person having ordinary skill in the art at the time

the invention was made to have modified Anderl et al. as modified, by the teachings of

Hastings et al. because wherein the data stored in the data storage media is encrypted, and

wherein the user authorization for the read access additionally comprises a decryption

key for the encrypted stored data would keep an unauthorized user from accessing the

files (see Hastings et al., column 5, lines 52-61).

Allowable Subject Matter

10.   Claims 29-39 are allowed.

Response to Amendments / Comments

11.   Applicant's comments filed on 5 December 2005 with respect to rejected claims

have been considered but are not deemed persuasive.

In response to the applicant's amendment directed towards the examiner's

suggestions, it is submitted that only claim 29 recites having the user table "separate from

said data storage media". The limitations added to claim 1, 15, and 40 only clarify that

the processor is separate from the data storage media, which as pointed out above is also

true of Anderl et al. also.

The examiner notes the applicant's characterizations of the Anderl et al. and

Smith references. The comments made toward these references do not appear to bring up

any arguments. The examiner has considered the applicant's position and these

comments have been entered into the file.

Conclusion

12.   Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Jacob F. Betit whose telephone number is (571) 272-

4075. The examiner can normally be reached on Monday through Friday 9:30 am to 5:30

pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Charles Rones can be reached on (571) 272-4085. The fax phone number for

the organization where this application or proceeding is assigned is 571-273-8300.

jfb
9 Jul 2006

SAM RIMELL
PRIMARY EXAMINER